Estimation of Decoy State Parameters for Practical QKD

1Sellami Ali, 2Omer Mahmoud and 2Rashid Abdelhaleem Saeed

1Department of Science in Engineering
2Department of Electrical and Computer Engineering Faculty of Engineering International Islamic University Malaysia

Abstract: We have presented a method to estimate parameters of the decoy state method based on one decoy state protocol for both BB84 and SARG04. This method has given different lower bound of the fraction of single-photon counts ($y_1$), the fraction of two-photon counts ($y_2$), the upper bound QBER of single-photon pulses ($e_1$), the upper bound QBER of two-photon pulses ($e_2$), and the lower bound of key generation rate for both BB84 and SARG04. The numerical simulation has shown that the fiber based QKD and free space QKD systems using the proposed method for BB84 are able to achieve both a higher secret key rate and greater secure distance than that of SARG04. Also, it is shown that bidirectional ground to satellite and inter-satellite communications are possible with our protocol.

Key words: Quantum cryptography, quantum key distribution, decoy state protocol and optical communications.

INTRODUCTION

The quantum key distribution (QKD) establishes secret keys shared between separated parties (i.e. Alice and Bob) to achieve secure communication in the presence of an eavesdropper (Eve). The QKD provides unconditional security, which is guaranteed by the fundamental laws of quantum physics (MAYERS, 2001). The QKD has been practically demonstrated over 175 km optical fiber (X.F. MO, et al., 2004), but with imperfect sources, noisy channels and inefficient detectors, which affect the security. In most of these cases the photon source is the coherent light, which is a superposition of Fock states weighted by Poisson distribution. In this respect, there is a nonzero probability to get a state with more than one photon (i.e. multi photon states). Thus Eve may suppress these states by keeping one photon. Precisely, Eve may block the single photon state, split the multi photon state and improve the transmission efficiency using her superior technologies to compensate the loss of the single photon. Therefore, any security proofs must take into account the possibility of subtle eavesdropping attacks, including the photon number splitting (PNS) attack (X. Ma,). A hallmark of those subtle attacks is that they introduce a photon-number dependent attenuation to the signal. Fortunately, it is still possible to obtain unconditionally secure QKD even with phase randomized attenuated laser pulses, as theoretically demonstrated by Gottesman-Lo-L"{u}tkenhaus-Preskill (GLLP) (H. Inamori,) as well as in (Gottesman, 2004). Nevertheless, there are limitations on the distance and the key generation rate (Koashi: quant-ph/0403131). These problems have been solved using the decoy state method introduced by Hwang (Hwang, 2003). The decoy state method achieves unconditional security based on quantum mechanics as well as improves dramatically the performance of the QKD. Also it faithfully estimates the upper bound of multi-photon counting rate through decoy–pulses regardless of the type attack. The basic idea of the decoy state QKD is: in addition to the signal state with the specific average photon number, on introduces some decoy states with some other average photon numbers and blends signal states with decoy states randomly in Alice’s sides. The decoy state QKD can be used to calculate the lower bound of counting rate of single-photon pulses and upper bound of quantum bit error rate (QBER) of bits generated by single-photon pulses. Many methods have been developed to improve the performance of the decoy states QKD, including more decoy states ( Wang, 2005), nonorthogonal decoy-state method (J.B. Li, 2006), photon number-resolving method (Qing-yu Cai, 2006), herald single photon source method (Tomoyuki Horikiri, 2006; Qin Wang, 2007), modified coherent state source method (Z.Q. Yin, 2007), the intensity fluctuations of the laser pulses (X.-B. Wang, 2007) and (X.-B.Wang, 2007). Some prototypes of decoy state QKD have been already implemented (Zhao, et al., 2006; Zhao, et al, 2006; Peng, et al., 2007; Rosenberg, 2007; Yuan, 2007; Tobias Schmitt-Manderbach et al., 2007; Yin et al., 2007).

Corresponding Author: Sellami Ali, Department of Science in Engineering
E-mail: sellami2003@hotmail.com

430
In this paper, we present one decoy state protocol and show more precisely how it can be used to estimate the lower bound of $y_1$ and upper bound of $e_1$ in order to get the final key generation rate of our QKD system for BB84 and to estimate the lower bound of fraction of two photon counts $y_2$ and upper bound of quantum bit-error rate (QBER) of two-photon $e_2$ for SARG04. We will introduce two factors $X$ and $Z$ which are factors for determining the lower bounds of the fraction of single-photon and two photon counts and the upper bounds of single-photon and two photons QBER. Next by using numerical simulation, we will compare the key generation rates and maximum secure distances of SARG04 and BB84 using our decoy states method.

This paper is prepared in the following order. In section II, we propose a tight verification of the fraction of the single photon state and the quantum bit error rate (QBER) for practical decoy method with one decoy state. In section III, we simulate the key generation rate over transmission distance. Also we investigate the maximization of the key generation rate by controlling the average photon numbers of signal state, decoy states and number of decoy state pulses. The main conclusions are summarized in section IV.

II. The Proposed Decoy State Method:

In this section, we show that in our estimation of the lower bound of fraction of single and two photon counts and upper bound of quantum bit-error rate (QBER) of single and two photon, we have used the same fiber based QKD system model (source, transmission, and detection) as that in (X. Ma,). It is assumed that Alice can prepare and emit a weak coherent state $\sqrt{\mu e^{i\theta}}$. Assuming the phase $\theta$ of each signal is randomized, the probability distribution for the number of photons of the signal state follows a Poisson distribution with some parameter $\mu$ (the intensity of signal states) which is given by $p_i = e^{-\mu} \frac{\mu^i}{i!}$, Alice’s pulse will contain $i$-photon. Therefore, it has assumed that any Poissonian mixture of the photon number states can be prepared by Alice. In addition, Alice can vary the intensity for each individual pulse.

The gain and QBER for signal state and one-decoy states are given by (X. Ma,).

\[
Q_\mu e^\mu = y_0 + \mu y_1 + \sum_{i=2}^{\infty} y_i \frac{\mu^i}{i!}
\]

\[
Q_\mu = y_0 + 1 - e^{-\mu}
\]

\[
E_\mu Q_\mu e^\mu = e_0 y_0 + e_i y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{\mu^i}{i!}
\]

\[
E_\mu = \frac{1}{Q_\mu} \left( e_0 y_0 + e_{\text{detector}} (1 - e^{-\mu}) \right)
\]

\[
Q_{y_1} e^{y_1} = y_0 + v_1 y_1 + \sum_{i=2}^{\infty} y_i \frac{v_1^i}{i!}
\]

\[
Q_{y_1} = y_0 + 1 - e^{-v_1}
\]

\[
E_{y_1} Q_{y_1} e^{y_1} = e_0 y_0 + e_i y_1 + \sum_{i=2}^{\infty} e_i y_i \frac{v_1^i}{i!}
\]

\[
E_{y_1} = \frac{1}{Q_{y_1}} \left( e_0 y_0 + e_{\text{detector}} (1 - e^{-v_1}) \right)
\]

Where $y_i$ is the yield of an $i$-photon state which comes from two parts, background ($v_0$) and true signal.
is the overall transmittance which is given by $\eta = \eta_{BoB} \frac{10^a}{10}$, where $a$ (dB/km) is the loss coefficient, $l$ is the length of the fiber and $\eta_{BoB}$ denotes for the transmittance in Bob’s side.

**Case 1 of one decoy state protocol for BB84:**

In this protocol, we should estimate the lower bounds of $y_1$ and the upper bounds of $e_1$. Intuitively, only one decoy state is needed for the estimation. Here, we investigate how to use one decoy state to estimate those bounds.

Suppose that Alice randomly changes the intensity of her pump light among 2 values (one decoy state and a signal state) such that the intensity of one mode of the two mode source is randomly changed among $V$ and $\mu$, which satisfy inequalities $0 < v < \mu < 1$, $0 < X < 1$, and $X > V/\mu$. Where, $V$ is the mean photon number of the decoy state and $\mu$ is the expected photon number of the signal state.

By using the inequality (8) in (Hwang, 2003), $0 < \mu < V_1 < V_2 < 1$ and $n \geq m$. We get

$$\sum_{i=2}^{\infty} y_i (P_i(v) - P_i(\mu)) \leq \left( \frac{P_2(v) - P_2(\mu)}{P_2(v)} \right)$$

Multiply both sides by $\sum_{i=2}^{\infty} \frac{y_i}{i!}$, we get

$$v_2 \left( \sum_{i=2}^{\infty} y_i \frac{v_i - \mu}{\mu} \right) \leq \left( v_1^2 - \mu^2 \right) \sum_{i=2}^{\infty} \frac{y_i}{i!}$$

According to Eq (1) we get

$$v_2^2 \left( Q_{v_2} e^v - Q_{\mu} e^\mu - (v_1 - \mu) y_1 \right) \leq \left( v_1^2 - \mu^2 \right) \left( Q_{v_1} e^{v_1} - y_0 - v_2 y_1 \right)$$

By solving inequality (4), the lower bound of $y_1$ is given by

$$y_1^{L,v,v_2} = \frac{1}{v_2^2 \left( v_1 - \mu \right) - (v_1^2 - \mu^2)} \left[ v_2^2 \left( Q_{v_2} e^v - Q_{\mu} e^\mu \right) - (v_1^2 - \mu^2)Q_{v_1} e^{v_1} + (v_1^2 - \mu^2) y_0 \right]$$

According to Eq. (1), then the lower bound of the gain of single photon state is given by

$$Q_1^{L,v,v_2} = \frac{\mu e^{-\mu}}{v_2^2 \left( v_1 - \mu \right) - (v_1^2 - \mu^2)} \left[ v_2^2 \left( Q_{v_2} e^v - Q_{\mu} e^\mu \right) - (v_1^2 - \mu^2)Q_{v_1} e^{v_1} + (v_1^2 - \mu^2) y_0 \right]$$

According to Eqs (1), we get

$$\sum_{i=2}^{\infty} e_i \frac{y_i}{i!} \geq \sum_{i=2}^{\infty} e_i \frac{v_i - \mu}{i!}$$

Then,

$$E_{v_1} Q_{v_2} e^{v_1} - e_0 y_0 - v_2 e_1 y_1 \geq \left( E_{v_1} Q_{v_2} e^{v_1} - E_{\mu} Q_{\mu} e^{\mu} - (v_1 - \mu) e_1 y_1 \right)$$

By solving inequality (8), the upper bound of $e_1$ is

$$e_1 \leq e_1^{U,v,v_2} = \frac{1}{v_2 - (v_1 - \mu)} \left[ E_{v_2} Q_{v_2} e^{v_2} - (E_{v_1} Q_{v_2} e^{v_1} - E_{\mu} Q_{\mu} e^{\mu}) - e_0 y_0 \right]$$
Case 2 of one decoy state protocol for SARG04:

In this protocol, I should estimate the lower bounds of \( y_2 \) and the upper bounds of \( e_2 \) in order to get the lower bound of key generation rate for SARG04. Intuitively, only one decoy state is needed for the estimation. Here, we investigate how to use one decoy state to estimate those bounds.

Suppose that Alice randomly changes the intensity of her pump light among 2 values (one decoy states and a signal state) such that the intensity of one mode of the two mode source is randomly changed among \( V \) and \( \mu \), which satisfy inequalities \( 0 < V < \mu < 1 \). Where, \( V \) is the mean photon number of the decoy state and \( \mu \) is the expected photon number of the signal state.

According to Eq. (1), the gain of signal and one decoy state are given by:

\[
Q_s e^\mu = y_0 + \mu y_1 + \frac{\mu^2}{2} y_2 + \sum_{i=3}^{\infty} y_i \frac{\mu^i}{i!} \\
Q_s e^\nu = y_0 + \nu y_1 + \frac{\nu^2}{2} y_2 + \sum_{i=3}^{\infty} y_i \frac{\nu^i}{i!}
\]

\[0 \leq V < \mu \leq 1, \quad (10)\]

Suppose Alice and Bob choose signal state and two decoy state with expected photon numbers \( \mu, V_1 \) and \( V_2 \) which satisfy

\[0 < V_1 + \mu < 1 \quad \text{and} \quad n \leq m. \quad (11)\]

By using Eq (1) and (2) we get

\[
\sum_{i=3}^{\infty} y_i \left( P_i(v_1) - P_i(\mu) \right) \leq \left( P_3(v_1) - P_3(\mu) \right) P_3(v_2) \quad (12)
\]

Multiply both sides by \( v_2^3 \sum_{i=3}^{\infty} \frac{y_i}{i!} \), we get

\[
v_2^3 \left( \sum_{i=3}^{\infty} \frac{y_i}{i!} \right) \left( v_1 - \mu^i \right) \leq \left( v_1 - \mu^i \right) \sum_{i=3}^{\infty} \frac{y_i}{i!} \quad (13)
\]

According to Eq (1) we found

\[
v_2^3 \left( Q_\nu e^{v_3} - Q_\sigma e^{\nu} - (v_1 - \mu) y_1 - \left( \frac{v_1^2 - \mu^2}{2} \right) y_2 \right) \\
\leq \left( v_1^3 - \mu^3 \right) \left( Q_\nu e^{v_3} - Q_\sigma e^{\nu} - (v_1^3 - \mu^3) y_0 \right)
\]

By solving inequality (14), the lower bound of \( y_2 \) is given by

\[
y_2 \geq y_2^{l,v_3,v_2} = \frac{2}{(v_1^2(v_1 - \mu) - (v_1^3 - \mu^3))v_2^2} \left[ v_2^3 \left( Q_\nu e^{v_3} - Q_\sigma e^{\nu} - (v_1^3 - \mu^3) y_1 \right) \\
- \left( v_2^3(v_1 - \mu) - (v_1^3 - \mu^3) v_2 \right) y_1 \right] \quad (15)
\]

According to Eq. (1), then the lower bound of the gain of single photon state is given by

\[
Q_{2^{l,v_3,v_2}} = \frac{\mu^2 e^{\nu} \left( v_2^3(v_1 - \mu) - (v_1^3 - \mu^3) v_2 \right)}{(v_1^2(v_1 - \mu) - (v_1^3 - \mu^3))v_2^2} \left[ v_2^3 \left( Q_\nu e^{v_3} - Q_\sigma e^{\nu} - (v_1^3 - \mu^3) y_0 \right)
- \left( v_2^3(v_1 - \mu) - (v_1^3 - \mu^3) v_2 \right) y_1 \right]
\]
According to Eqs (1), and (10) we get

\[
\sum_{i=3}^{\infty} e_i y_i \frac{v_i^2}{l!} \geq \sum_{i=3}^{\infty} e_i y_i \frac{v_i^2 - \mu_i^2}{l!}
\]

Then,

\[
E_n Q_n e^v - e_0 y_0 - v_2 e_1 y_1 - \frac{v_2^2}{2} e_2 y_2 \geq \left( E_n Q_n e^v - E_n Q_n e^v - e_2 y_2 - (v_i - \mu_i) e_i y_i - \frac{v_i^2 - \mu_i^2}{2} e_i y_i \right)
\]

By solving inequality (18), the upper bound of \( e_i \) is

\[
e_i \leq \frac{2}{(v_i^2 - (v_i - \mu_i)^2)} \frac{1}{y_i^2} - (v_i - (v_i - \mu_i) e_i y_i + e_i y_i)
\]

After estimating the lower bounds of \( y_1 \) and \( y_2 \) and the upper bounds of \( e_1 \) and \( e_2 \) for each decoy state protocol. Then, we can use the following formula to calculate the final key generation rate of our QKD system for both BB84 and SARG04 protocols (X. Ma,) and (C.-H. Fung, 2006) respectively:

\[
R_{BB84} \geq R_{BB84}^L = q \{ -Q_\mu f (E_\mu) H_2 (E_\mu) + Q_1^L \} \[ 1 - H_2 (e_1^U) \]
\]

\[
R_{SARG04} \geq R_{SARG04}^L = -Q_\mu f (E_\mu) H_2 (E_\mu) + Q_1^L \} \[ 1 - H_2 (e_1^U) \] + Q_2^L \[ 1 - H_2 (e_2^U) \]
\]

where q depends on the implementation (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol (H.K. Lo, 2004), q=1)f(x) is the bi-direction error correction efficiency as a function of error rate, normally f(x) ≥ 1 with Shannon limit f(x) = 1, and H_2(x) is binary Shannon information function having the form H_2(x) = -x log2 (x) - (1-x) log2 (1-x).

III. Numerical Results:
Fiber Based QKD System Simulation:

In this section, we discuss the numerical simulation which is important for setting optimal experimental parameters and choosing the distance to perform certain decoy method protocol. The principle of numerical simulation is that for certain QKD set-up, if the intensities, percentages of signal state and decoy states are known, we could simulate the gains and QBERs of all states. This is the key point in the experiment. More precisely, we evaluate the values of the gain of signal states \( Q_\mu \), the gain of decoy states \( Q_n \), the overall quantum bit error rate (QBER) for signal states \( E_\mu \), and for decoy states \( E_n \), and then calculate the lower bound of the fraction of single (\( y_1 \)) and two photon counts (\( y_2 \)), the upper bound QBER of single (\( e_1 \)) and two photon pulses (\( e_2 \)), and then substitute these results into Eq. (44,45) for getting the lower bound of key generation rate.

First, we try to simulate an optical fiber based QKD system using our decoy state method for both BB84 and SARG04, the losses in the quantum channel can be derived from the loss coefficient \( \alpha \) in dB/km and the length of the fiber l in km. the channel transmittance can be written as \( \eta_{dB} = 10^{\frac{-\alpha l}{10}} \), and the overall transmission between Alice and Bob is given by \( \eta = \eta_{\text{Bob}} \eta_{AB} \) where \( \alpha = 0.2 \) dB/km our set-up is the loss coefficient, \( \eta_{\text{Bob}} \) is the transmittance in Bob’s side. We choose the detection efficiency of \( \eta = 4.5 \times 10^{-5} \), detectors dark count rate of \( y_0 = 1.7 \times 10^{-4} \), the probability that a photon hits the erroneous detector (\( e_{\text{det}} = 0.033 \)), the wavelength (\( \lambda = 1550nm \)), the data size is \( N = 6 \times 10^9 \). These parameters are taken from the GYS experiment (Gobby, 2004). we choose the intensities, the percentages of signal state and decoy states which could give out the optimization of key generation rate and the maximum secure distance for the protocols which are proposed. The search for optimal parameters can be obtained by numerical simulation.
Figure (1) illustrates the simulation results of the key generation rate against the secure distance of fiber link for different decoy state protocols with statistical fluctuation. (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^2} \). (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^3} \). (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^4} \). (e) The asymptotic decoy state method (with infinite number of decoy states) for both single and two photons contributions (SARG04). (f) The asymptotic decoy state method (with infinite number of decoy states) for only single photon contributions (SARG04). (g) The key generation rate of one decoy state protocol with the statistical fluctuations (SARG04) when \( x = 1 \). Comparing these curves, it can be seen that the fiber based QKD system using the proposed method for BB84 is able to achieve both a higher secret key rate and greater secure distance than SARG04. The maximal secure distances of the five curves are 142 km, 123.5 km, 122.2 km, 121.3 km, 97 km, 94 km, and 71 km.

**Fig. 1:** The simulation results of the key generation rate against the secure distance of fiber link for different decoy state protocols for BB84 and SARG04. (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^2} \). (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^3} \). (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{V}{\mu^4} \). (e) The asymptotic decoy state method (with infinite number of decoy states) for both single and two photons contributions (SARG04). (f) The asymptotic decoy state method (with infinite number of decoy states) for only single photon contributions (SARG04). (g) The key generation rate of one decoy state protocol with the statistical fluctuations (SARG04) when \( x = 1 \).

**Free Space QKD System Simulation:**

Next, we draw the attention to simulate a free space QKD system using our decoy state method for both SARG04 and BB84. We assume that conventional telescope architectures, like the Cassegrain type, are used both in the transmitting and receiving sides. They are reflective telescopes, in which the secondary mirror produces a central obscuration. Moreover, their finite dimensions and the distance between them are responsible of the beam diffraction. The attenuation due to beam diffraction and obscuration can be expressed as
\[ \eta_{\text{diff}} = \eta_{\text{diff}} \eta_{\text{diff}} \]

\[ \eta_{\text{diff}} = \exp \left[ -\frac{2 \left( D_{M1} \right)^2}{w^2} \right] - \exp \left[ -\frac{2 \left( D_{M2} \right)^2}{w^2} \right] \]

\[ \eta_{\text{diff}} = \exp \left[ -\frac{2 \left( D_{M1} \right)^2}{w^2} \right] - \exp \left[ -\frac{2 \left( D_{M2} \right)^2}{w^2} \right] \]

\[ w \approx \frac{\lambda L}{\pi W_0} \] (22)

where the subscript \( t \) refers to the transmit telescope and \( r \) to the receive one. \( \lambda \) is the wavelength, and \( D_{M1} \) and \( D_{M2} \) are the radius of the primary and secondary mirrors, respectively. \( W \) is the waist radius of the Gaussian beam and \( L \) is the distance between the telescopes.

Since the atmospheric attenuation (\( \eta_{\text{atm}} \)) is produced by three phenomena: scattering, absorption and turbulence, it can be expressed as \( \eta_{\text{atm}} = \eta_{\text{scat}} \eta_{\text{abc}} \eta_{\text{turb}} \). The light is absorbed and scattered by the gas molecules and the aerosols when it passes through the atmosphere. However, the most relevant contribution to the atmospheric attenuation is caused by the turbulence, which is due to thermal fluctuations that produce refractive index variations. The turbulence depends basically on the atmospheric conditions and the position of the ground station. Finally, the total channel attenuation can be written as

\[ \eta = \eta_{\text{diff}} \eta_{\text{atm}} \eta_{\text{det}} \] (23)

The assumed link parameters are the wavelength \( \lambda = 650 \text{nm} \) corresponds to an absorption window and the 0.65 efficiency peak of the chosen detector (an SPCM-AQR-15 commercial silicon avalanche photodiode detector) with \( 1.7 \times 10^4 \text{ counts/pulse} \) dark counts. The satellite telescopes radius of the primary and secondary mirrors are 15 cm and 1cm, respectively. The ground telescopes radius of the primary and secondary mirrors are 50 cm and 5cm, respectively. The values of telescopes radii have been obtained from the SILEX Experiment (Gatenby, 1991) and the Tenerife’s telescope (Ursin. et al., 2007). The uplink attenuation due to turbulence has been computed considering the Tenerife’s telescope (\(-3 \text{km above sea level}\)) for two conditions: 1 hour before sunset (\( \eta_{\text{atm}}=5 \text{dB} \)) and a typical clear summer day (\( \eta_{\text{atm}}=1 \text{dB} \)) (Aviv, 2006). The turbulence effect on the downlink is negligible. The scattering attenuation is evaluated using a model of Clear Standard Atmosphere (L. Elterman, 1964), which results in \( (\eta_{\text{atm}}=1 \text{dB}) \).

By simulating the different scenarios, we found the curves with similar shapes. They illustrate the simulation results of the key generation rate against the transmission distance for both BB84 and SARG04 protocols as shown in Figures (2-5). The distances in the downlink are significant larger compared to the uplink thanks to the lack of turbulence attenuation: In fact, MEO satellite downlink communication using our estimations is possible. This increase in distance is not achieved in the intersatellite link due to the reduced telescope dimensions. The most relevant parameters that influence the critical distance are the turbulence attenuation and the telescopes dimensions. Therefore, bidirectional ground-to-LEO satellite communication is possible with our estimations. Comparing these results, it can be seen that the fiber based and satellite based QKD system using the proposed method for BB84 is able to achieve both a higher secret key rate and greater secure distance than SARG04. This lead to say that the two-photon part has a small contribution to the key generation rates at all distances.

**Conclusion:**

In conclusion, we have presented an efficient and feasible decoy-state method to implement fiber-based QKD and free space QKD systems over very lossy channels for both BB84 and SARG04. We have clearly demonstrated how to estimate the lower bound of the fraction of single-photon counts (\( y_1 \)), the fraction of two-photon counts (\( y_2 \)), the upper bound QBER of single-photon pulses (\( e_1 \)), the upper bound QBER of two-photon pulses (\( e_2 \)), and to evaluate the lower bound of key generation rate for both BB84 and SARG04. Our results show that the fiber based QKD and free space QKD systems using the proposed method for BB84 is able to achieve both a higher secret key rate and greater secure distance than that of SARG04. Hence, the two-photon
part has a small contribution to the key generation rates at all distances. Also, our results show that bidirectional ground to satellite and inter-satellite communications are possible using our protocol.

![Graph](image1)

**Fig. 2:** A satellite-ground downlink. The key generation rate against the transmission distance link (km). (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $x = \frac{\sqrt{2}}{\mu}$. (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $x = \frac{\sqrt{2}}{\mu^2}$. (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $X=1$. (e) The asymptotic decoy state method (with infinite number of decoy states) for both single and two photons contributions (SARG04).

![Graph](image2)

**Fig. 3:** An inter-satellite link. The key generation rate against the transmission distance link (km). (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $x = \frac{\sqrt{2}}{\mu}$. (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $x = \frac{\sqrt{2}}{\mu^2}$. (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when $X=1$. 

437
Fig. 4: A ground-satellite uplink 1 hour before sunset (\( \eta_{\text{turb}} = 5 \text{dB} \)). The key generation rate against the transmission distance link (km). (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{v}{\mu^2} \). (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{v}{\mu} \). (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( X = 1 \).

Figure 5: A ground-satellite uplink during a typical clear summer day (\( \eta_{\text{turb}} = 5 \text{dB} \)). The key generation rate against the transmission distance link (km). (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{v}{\mu^2} \). (c) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( x = \frac{v}{\mu} \). (d) The key generation rate of one decoy state protocol with the statistical fluctuations (BB84) when \( X = 1 \).
REFERENCES

Lett., 84: 3762.
Zhao, Yi., et al., 2006. Proceedings of IEEE International Symposiumon Information Theory, PP: 2094-
2098.